ELLIOT ENOKI #1528
Acting United States Attorney
District of Hawaii

LAWRENCE L. TONG #3040
Chief, Fraud and Financial Crime Section

KENNETH M. SORENSON
MARC A. WALLENSTEIN #10456
Assistant U.S. Attorneys
Room 6100, PJKK Federal Building
300 Ala Moana Blvd.
Honolulu, Hawaii 96850
Telephone: 541-2850
Facsimile: 541-2958
E-mail: ken.sorenson@usdoj.gov
marc.wallenstein@usdoj.gov

TARYN M. MEEKS
Trial Attorney
Counterterrorism Section
National Security Division
U.S. Department of Justice
950 Pennsylvania Ave. NW
Washington, D.C. 20530

Attorneys for Plaintiff
UNITED STATES OF AMERICA

IN THE UNITED STATES DISTRICT COURT FOR THE

DISTRICT OF HAWAII

UNITED STATES OF AMERICA, Plaintiff, v. IKAIKA ERIK KANG, Defendant.	Cr. No. 17-00446 SOM-KJM **JOINT MOTION FOR PROTECTIVE ORDER REGARDING CLASSIFIED INFORMATION**

JOINT MOTION FOR PROTECTIVE ORDER REGARDING CLASSIFIED INFORMATION

The parties jointly and respectfully move this Court, pursuant to the authority granted under Section 3 of the Classified Information Procedures Act, 18 U.S.C. App. III (CIPA); the Security Procedures established pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA § 9) (hereinafter the "Security Procedures"); the general supervisory authority of the Court; and to protect the national security, to enter the attached proposed Protective Order regarding the disclosure and dissemination of classified national security information that will be made available to the defense by the Government.

The definition of classified information is established by Executive Order and statute, *see* CIPA § 1(a) (defining classified information as "any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security"); Exec. Order 13526 § 1.1(a) (defining classification standards), and the government unilaterally determines what constitutes classified information. *See United States v. Smith*, 750 F.2d 1215, 1217 (4th Cir. 1984) ("It is apparent, therefore,

that the government pursuant to the authority mentioned in section 1 may determine what information is classified. A defendant cannot challenge this classification. A court cannot question it.”). The attached Order details protections and procedures. The parties request that the Court enter a protective order in this case with respect to items turned over to the defendant in discovery.

Respectfully submitted this 21st day of September, 2017.

ELLIOT ENOKI
Acting United States Attorney
District of Hawaii

/s/ Kenneth Sorenson
KENNETH SORENSON
Assistant United States Attorney

/s/ Marc A. Wallenstein
MARC A. WALLENSTEIN
Assistant United States Attorney

/s/ Marc A. Wallenstein *for*
TARYN MEEKS
National Security Division
U.S. Department of Justice

/s/ Birney Bervar
BIRNEY BERVAR
Attorney for Defendant
IKAIKA ERIK KANG

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on the dates and by the methods of service noted below, a true and correct copy of the foregoing was served on the following at their last known addresses:

Served by U.S. mail:

BIRNEY B. BERVAR, ESQ.
bbb@bervar-jones.com

Attorney for Defendant
IKAIKA ERIK KANG

DATED: September 21, 2017, at Honolulu, Hawaii.

/s/ Anika Ramos
U.S. Attorney's Office
District of Hawaii

IN THE UNITED STATES DISTRICT COURT FOR THE

DISTRICT OF HAWAII

UNITED STATES OF AMERICA, Plaintiff, v. IKAIKA ERIK KANG, Defendant.	Case No. 1:17-cr-00446-SOM PROTECTIVE ORDER REGARDING CLASSIFIED INFORMATION

PROTECTIVE ORDER REGARDING CLASSIFIED INFORMATION

This matter comes before the Court upon the parties' Joint Motion for Protective Order to prevent the unauthorized use, disclosure or dissemination of classified national security information and documents, and other discovery materials, that will be reviewed by or made available to, or are otherwise in the possession of, defense counsel in this case.

Pursuant to the authority granted under section 3 of the Classified Information Procedures Act, 18 U.S.C. App. III ("CIPA"); the Security Procedures established pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA § 9) (hereinafter the "Security Procedures"); the Federal Rules of Criminal Procedure 16(d) and 57; the general

supervisory authority of the Court; and, in order to protect the national security, the parties' joint motion is GRANTED.

IT IS HEREBY ORDERED:

1. The Court finds that this case will involve classified national security information, the storage, handling, and control of which, by law or regulation, require special security precautions, and access to which requires a security clearance and a need-to-know.

2. The purpose of this Protective Order ("Order") is to establish the procedures that must be followed by all defense counsel of record, their designated employees and agents, translators, experts, and investigators for the defense, all other counsel involved in this case, and all other individuals who receive access to classified information or documents in connection with this case.

3. The procedures set forth in this Order shall apply to all pre-trial, trial, post-trial, and appellate stages of this case; and may be modified from time to time by further order of the Court acting under this Court's inherent supervisory authority to ensure a fair and expeditious trial.

Definitions

4. As used herein, the terms "classified national security information and documents," "classified information," "classified documents," and "classified material" refer to:

A. Any classified document or information that has been classified by any Executive Branch agency in the interest of national security or pursuant to Executive Order 13526 or its predecessor orders as “CONFIDENTIAL,” or “SECRET,” or “TOP SECRET,” or “SENSITIVE COMPARTMENTED INFORMATION (“SCI”)”; or any information contained in such documents;

B. Any document or information, regardless of its physical form or characteristics, now or formerly in the possession of a private party, which has been derived from a United States Government classified document, information, or material, regardless of whether such document, information, or material has itself subsequently been classified by the Government pursuant to Executive Order 13526 or its predecessor orders as “CONFIDENTIAL” or “SECRET,” or “TOP SECRET,” or “SCI;”

C. Oral information known to the defense counsel to be classified;

D. Any document or information, including oral information, which the defense counsel have been notified orally or in writing contains classified information;

E. Any information, regardless of place or origin and including “foreign government information” as that term is defined in Executive Order 13526, that could reasonably be believed to contain classified information; and

F. Any information obtained from an agency that is a member of the United States "Intelligence Community" (as defined in section 3(4) of the National Security Act of 1947, codified at 50 U.S.C. § 401a(4)), that could reasonably be believed to contain classified information or that refers to national security or intelligence matters.

5. The disclosure or provision of documents or materials by the government to the defendant shall not operate as a waiver of any privilege or protection that could or may be asserted by the holder of any such privilege or protection.

6. The words "documents," "information," and "material" shall include but are not limited to all written or printed matter of any kind, formal or informal, including originals, conforming copies and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise), and further include but are not limited to:

A. Papers, correspondence, memoranda, notes, letters, reports, summaries, photographs, maps, charts and graphs, interoffice and intra-office communications, notations of any sort concerning conversations, meetings or other communications, bulletins, teletypes, telegrams and telefacsimiles, invoices, worksheets and drafts, alterations, modifications, changes, and amendments of any kind to the foregoing;

B. Graphic or oral records or representations of any kind, including but not limited to photographs, charts, graphs, microfiche, microfilm, videotapes, sound recordings of any kind, and motion pictures;

C. Electronic, mechanical or electric records of any kind, including but not limited to tapes, cassettes, disks, recordings, films, typewriter ribbons, word processing or other computer tapes or disks, and all manner of electronic data processing storage; and

7. "Access to classified information" means having access to, reviewing, reading, learning or otherwise coming to know in any manner any classified information.

8. "Secure Area" shall mean a sensitive compartmented facility or other appropriate facility approved by a Classified Information Security Officer for storage, handling, and control of classified information.

9. All classified documents or material and the information contained therein shall remain classified unless the documents or material bear a clear indication that they have been declassified by the agency or department that is the originating agency (hereinafter the "Originating Agency") of the document, material, or information contained therein.

10. Any classified information provided to the Defense by the Government is to be used solely by the Defense and for the

purpose of preparing the defense. The Defense may not disclose or cause to be disclosed in connection with this case any information known or reasonably believed to be classified information except as otherwise provided herein.

11. *Classified Information Security Officer*. In accordance with the provisions of CIPA and the Security Procedures, the Court designates, Winfield S. "Scooter" Slade as Classified Information Security Officer ("CISO"), and designates Debra M. Guerrero-Randall, Daniel O. Hartenstine, Joan B. Kennedy, Shawn P. Mahoney, Maura L. Peterson, Carli V. Rodriguez-Feo, and Harry J. Rucker as alternate-classified information security officers, for the purpose of providing security arrangements necessary to protect from unauthorized disclosure any classified information to be made available in connection with this case. Defense counsel shall seek guidance from the CISO with regard to appropriate storage, handling, transmittal, and use of classified information.

12. *Government Attorneys*. The Court has been advised that the Government attorneys working on this case, Assistant United States Attorney Ken Sorenson and Marc Wallenstein, and U.S. Department of Justice Attorney Taryn Meeks, and their respective supervisors (collectively referred to hereinafter as the "Government Attorneys"), have the requisite security clearances

to have access to the classified information that relates to this case.

13. *Protection of Classified Information*. The Court finds that, in order to protect the classified information involved in this case, only certain persons associated with the defense may have access to the classified information in this case, as set forth below in Paragraphs 14-16.

14. *Defense Counsel*. Subject to the provisions of paragraph 15, the following attorney for the defense may be given access to classified information as required by the Government's discovery obligations: Birney Bervar, who the Court has been advised has the appropriate security clearance.

15. *Defense personnel*. Defense counsel, defense translators, and defense investigators, and defense experts working on this case (collectively, "the Defense"), may obtain access to classified documents or information only if such persons have:

1) Received the necessary security clearance at the appropriate level of classification, through or confirmed by the CISO; and

2) Signed the Memorandum of Understanding in the form attached hereto, agreeing to comply with the terms of this Order. Defense counsel shall file originals of the executed Memoranda of Understanding with the Court under

seal and serve copies of such document upon the CISO and the Government.

16. Any additional person whose assistance the Defense reasonably requires may have access to classified information in this case only after obtaining from the CISO an approval for access to the appropriate level of classification on a need-to-know basis, and after satisfying the other requirements described in this Order for access to classified information, including those set forth in Paragraph 15.

17. The substitution, departure, and removal for any reason from this case of counsel for the defendant, or anyone associated with the defense as an employee or otherwise, shall not release that person from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

18. Unless they already hold an appropriate security clearance and are approved for access to classified information in this case, the Defense, including all persons whose assistance the Defense reasonably requires, shall complete and submit to the CISO a Standard Form 86 (“Security Investigation Data for Sensitive Position”), attached releases, and “major case” fingerprints in order to obtain security clearances necessary for access to classified information that may be involved in this case. The CISO shall provide access to the necessary forms. The CISO shall take

all reasonable steps to process all security clearance applications.

19. *Special procedures for audio recordings.* Any classified audio recordings that the government discloses to the defense shall be maintained by the CISO in the Secure Area. Such recordings may only be reviewed on a stand-alone, non-networked computer or other device within the Secure Area of Review that does not have the capability to duplicate or transmit information.

20. *Secure Area of Review*. The CISO shall arrange for an appropriately approved Secure Area for use by the Defense. The CISO shall establish procedures to assure that the Secure Area is reasonably accessible to the Defense. The Secure Area will be outfitted with any secure office equipment requested by the Defense that is reasonable and necessary to the preparation of the defense in this case. The CISO, in consultation with defense counsel, shall establish procedures to assure that the Secure Area may be maintained and operated in the most efficient manner consistent with the protection of classified information. No documents or other material containing classified information may be removed from the Secure Area unless authorized by the CISO. The CISO shall not reveal to the Government the content of any conversations he or she may hear among the Defense, nor reveal the nature of documents being reviewed by them, nor the work generated by them.

In addition, the presence of the CISO shall not operate to waive, limit, or otherwise render inapplicable, the attorney-client privilege.

21. *Filings with the Court*. Until further order of this Court, any motion, memorandum, or other document filed by the Defense that defense counsel knows, or has reason to believe, contains classified information, in whole or in part, or any document the proper classification of which defense counsel is unsure, shall be filed under seal with the Court through the CISO or an appropriately cleared designee of his choosing. Pleadings filed under seal with the CISO shall be marked "Filed In Camera and Under Seal" with the CISO and shall include in the introductory paragraph a statement that the item is being filed under seal pursuant to this Order, but need not be accompanied by a separate motion to seal. The date and time of physical submission to the CISO or a designee shall be considered as the date and time of court filing. At the time of making a physical submission to the CISO or a designee, counsel shall file on the public record in the CM/ECF system a notice of filing. The notice should contain only the case caption and an unclassified title in the filing. The CISO shall make arrangements for prompt delivery under seal to the Court and counsel for the Government any document to be filed by the Defense that contains classified information. The CISO shall promptly examine the document and, in consultation with

representatives of the appropriate Government agencies, determine whether the document contains classified information.

22. Any document filed by the Government containing classified information shall be filed under seal with the Court through the CISO or an appropriately cleared designee of his choosing. Pleadings filed under seal with the CISO shall be marked "Filed In Camera and Under Seal with the Court Information Security Officer" and shall include in the introductory paragraph a statement that the item is being filed under seal pursuant to this Order, but need not be accompanied by a separate motion to seal. The date and time of physical submission to the CISO or a designee, which should occur no later than 4:00pm, shall be considered the date and time of filing. The CISO shall make arrangements for prompt delivery under seal to the Court and defense counsel (unless ex parte) any document to be filed by the Government that contains classified information. At the time of making a physical submission to the CISO or a designee, counsel shall file on the public record in the CM/ECF system a notice of filing. The notice should contain only the case caption and an unclassified title in the filing.

23. *Sealing of Records*. The CISO shall maintain a separate sealed record for those pleadings containing classified information, and retain such record for purposes of later proceedings or appeal.

24. Access to Classified Information. The Defense shall have access to classified information only as follows:

A. All classified information produced by the Government to the Defense, in discovery or otherwise, and all classified information possessed, created or maintained by the Defense, shall be stored, maintained and used only in the Secure Area established by the CISO;

B. The Defense shall have free access to the classified information made available to them in the Secure Area, and shall be allowed to take notes and prepare documents with respect to those materials. However, the Defense shall not disclose the classified information, either directly, indirectly, or in any other manner that would disclose the existence of such, without following the procedures for use and disclosure of classified information through the CISO. If the defense is unsure whether pursuing a particular defense might reveal classified information to persons not authorized to receive it, the defense should consult the CISO.

C. The Defense shall not copy or reproduce any classified information in any form, except with the approval of the CISO, or in accordance with the procedures established by the CISO for the operation of the Secure Area;

D. All documents prepared by the Defense (including, without limitation, pleadings or other documents intended for

filing with the Court) that do or may contain classified information, shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons who have received an appropriate approval for access to classified information, and in the Secure Area on equipment approved for the processing of classified information, and in accordance with the procedures established by the Court Information Security Officer. All such documents and any associated materials (such as notes, drafts, copies, compact discs, DVDs, thumb drives, and any other electronic or non-electronic media) containing classified information shall be maintained in the Secure Area, unless and until the CISO determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to counsel for the Government;

E. The Defense shall discuss classified information only within the Secure Area or in another area authorized by the CISO, and shall not discuss or attempt to discuss classified information over any standard commercial telephone instrument or office intercommunication system; and

F. The Defense shall not disclose any classified information to any person not authorized pursuant to this Order, including the defendant and defense witnesses, the Court, court personnel, and the Government Attorneys who have been identified by the CISO as having the appropriate clearances and the need-to-

know that information. Any person approved by the CISO for disclosure under this paragraph shall be required to obtain the appropriate security clearance, to sign and submit to the Court the Memorandum of Understanding appended to this Order, and to comply with all terms and conditions of this Order. If preparation of the Defense requires that classified information be disclosed to persons not named in this Order, then, upon approval by the CISO, the CISO shall promptly seek to obtain security clearances for them at the request of defense counsel.

25. Information that is classified that also appears in the public domain is not thereby automatically declassified unless it appears in the public domain as the result of an official statement by a U.S. Government Executive Branch official who is authorized to declassify the information. Individuals who by virtue of this Order or any other court order are granted access to the classified information may not confirm or deny classified information that appears in the public domain. Prior to any attempt by the Defense to have such information confirmed or denied at trial or in any public proceeding in this case, the Defense must comply with the notification requirements of section 5 of CIPA and all the provisions of this Order.

26. In the event that any classified information enters the public domain, the Defense is precluded from making private or public statements where the statements would reveal personal

knowledge from non-public sources regarding the classified status of the information, or would disclose that the Defense had personal access to classified information, contradicting, or otherwise relating to the information already in the public domain. The Defense is not precluded from citing or repeating information in the public domain that counsel does not know or have reason to believe to be classified information, or derived from classified information.

27. Procedures for the use or disclosure of classified information by the Defense shall be those provided in sections 5 and 6 and 8 of CIPA. To facilitate the Defense's filing of notices required under section 5 of CIPA, the CISO shall make arrangements with the appropriate agencies for a determination of the classification level, if any, of materials or information, either within the possession of the Defense or about which the Defense has knowledge and which the Defense intends to use in any way at any pre-trial proceeding, deposition or at trial. Nothing submitted by the Defense to the CISO pursuant to this paragraph shall be made available to counsel for the Government unless so ordered by the Court, or so designated by the Defense. Any and all items that are classified shall be listed in the defendant's CIPA section 5 notice. To the extent that any classified information is the basis of any motion filed by the Defense, such motion shall be preceded by a CIPA section 5 notice.

28. Any individual subject to this Order who is not certain whether information is classified should consult with the CISO.

29. All classified information to which the Defense has access in this case is now and will remain the property of the United States. The defense counsel, defense counsel employees, defense translators, investigators, experts, and anyone else who receives classified information pursuant to this Order shall return all such classified information in their possession obtained through discovery from the Government in this case, or for which they are responsible because of access to classified information, to the CISO upon request. The notes, summaries and other documents prepared by the Defense that do or may contain classified information shall remain at all times in the custody of the CISO for the duration of this case. At the conclusion of all proceedings, including any final appeals, all such notes, summaries and other documents are to be destroyed by the CISO in the presence of defense counsel if so desired.

30. *Violations of this Order*. Unauthorized use or disclosure of classified information may constitute violations of United States criminal laws. In addition, violation of the terms of this Order shall be immediately brought to the attention of the Court, and may result in a charge of contempt of Court and possible referral for criminal prosecution. Any breach of this Order may result in the termination of a person’s access to classified

information. Persons subject to this Order are advised that direct or indirect unauthorized use, disclosure, retention or negligent handling of classified information could cause serious damage, and in some cases exceptionally grave damage, to the national security of the United States, or may be used to the advantage of a foreign nation against the interests of the United States. This Order is to ensure that those authorized by the Order to receive classified information will never divulge the classified information disclosed to them to anyone who is not authorized to receive it, or otherwise use the classified information, without prior written authorization from the Originating Agency and in conformity with this Order.

31. Nothing in this Order shall preclude the Government from seeking a further protective order pursuant to CIPA and/or Rule 16(d) of the Federal Rules of Criminal Procedure as to particular items of discovery material, or the handling of unclassified discovery generally.

32. A copy of this Order shall be issued forthwith to counsel for the defendant, who shall be responsible for advising the

defendant and defense counsel employees, translators, experts, investigators, and all other defense personnel of the contents of this Order.

SO ORDERED this _____ day of September 2017.

_____
HONORABLE SUSAN OKI MOLLWAY
UNITED STATES DISTRICT COURT JUDGE

USA v. Ikaika Erik Kang,
Cr. No. 17-00446 SOM-KJM
"Protective Order Regarding Classified Information"